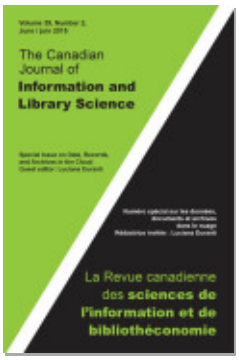
# What About Trust in the Cloud? Archivists' Views on Trust / La question de la confiance dans le nuage: Le point de vue des archivistes sur la question

Erik A.M. Borglund




Canadian Journal of Information and Library Science, Volume 39, Number 2, June juin 2015, pp. 114-127 (Article)

Published by University of Toronto Press
*DOI:* *https://doi.org/10.1353/ils.2015.0017*

# What About Trust in the Cloud? Archivists' Views on Trust

# La question de la confiance dans le nuage : Le point de vue des archivistes sur la question

Erik A.M. Borglund
Mid Sweden University
erik.borglund@miun.se

Abstract: More and more information is "going to the cloud," including records and archives. This article focuses on understanding trust-in-cloud solutions from an archivist's perspective, exploring whether cloud computing has changed the archivist's role and how archivists respond to cloud-related problems and challenges. Twelve archivists in Sweden were interviewed in Swedish. They describe changes in their role due to cloud computing and services in the domain of archival science. Their role has changed from being reactive to becoming proactive, guarding not only the organization's needs and assets but also its archival records. Working proactively implies guaranteeing that requirements are updated and that contracts and agreements between the organization and cloud service provider are correct. The research shows that trust consists of several dimensions and cannot be easily achieved with technical solutions. Organizations' risk-tolerance levels have also changed to take advantage of the benefits and savings that cloud services provide for organizations.

Keywords: archivists, cloud computing, records, trust

Résumé : Des quantités de plus en plus importantes d'information vont « dans le nuage », y compris des dossiers d'archives. Cet article se propose de comprendre le point de vue des archivistes concernant la confiance qui peut être accordée aux solutions informatiques en nuage, d'examiner si l'informatique en nuage a changé le rôle des archivistes et comment les archivistes réagissent aux problèmes et aux défis liés aux nuages informatiques. Douze archivistes en Suède ont été interrogés en suédois. Ils décrivent les changements dans leur rôle dûs à l'informatique en nuage et dans les services propres au domaine de l'archivistique. Leur rôle est passé de réactif à proactif, se faisant les gardiens des besoins et des actifs de leur organisation, et non seulement de ses documents d'archives. Travailler de manière proactive implique de garantir que les exigences sont mises à jour, et que les contrats et les accords entre l'organisation et le fournisseur de service informatique en nuage sont corrects. La recherche montre que la confiance se compose de plusieurs dimensions, et qu'elle ne peut pas être facilement réalisée avec des solutions techniques. Les niveaux de tolérance au risque des organisations ont également changé, afin de tirer profit des avantages et des économies que les services d'informatique en nuage apportent aux organisations.

Mots-clés : archivistes, informatique en nuage, documents, confiance

## Introduction

In the last couple of years, more and more information is "going to the cloud," including records and archives, yet very little research has been undertaken to assess the impact of cloud computing from an archival science perspective (Ferguson-Boucher and Convery 2011). "The cloud" is the short term for cloud computing, a metaphor for various services available through a network, which, in most cases, is the Internet. In cloud computing, a range of different computing resources may be accessed, and one way to present and understand the cloud is to use the model defined by the US National Institute of Standards and Technology (NIST) (National Institute of Standards and Technology 2009; Mell and Grance 2011). Service models are central to the NIST model: software as a service (SaaS); platform as a service (PaaS); and infrastructure as a service (IaaS).

As a result of its low cost, organizations are increasingly moving their records into the cloud and delegating to cloud providers the responsibility for their security, accessibility, disposition, and preservation. However, how high is the price that these organizations pay in terms of having control over their records or, as is the case with archives, of the records entrusted to them for permanent preservation? We have seen cloud providers go bankrupt, disappear, or be sold; records lost, retained when they should have been destroyed, or mixed up in shared servers; failed back-ups; and unauthorized access by sub-contractors and hackers. Further, it is impossible to pinpoint the geographical location of the records at any given time as well as the jurisdiction under which they fall; to prove the chain of custody and the authenticity of the records; to ensure protection of legal privilege or trade secrets when using a third party; to isolate documents for legal hold; to conduct audits; and to guarantee that the records that need to be permanently preserved are kept according to archival standards. These are only a few of the problems encountered by organizations using the cloud as if it were a recordkeeping or a record-preservation system. Yet the number of those who choose to use the cloud for these purposes is growing exponentially by the day. If this phenomenon cannot be stopped, we must at least try to reduce its risks to an acceptable level.

In the existing literature about archives and the cloud, several different focuses and trends can be identified. There are examples of archives being presented as cloud solutions and of the archive being presented as a service (Askhoj, Nagamori, and Sugimoto 2011; Askhoj, Sugimoto, and Nagamori 2011). However, a literature search in scientific bibliographic databases and outlets found nothing about electronic archives being developed using PaaS or IaaS, which are similar to more traditional outsourcing. Another identifiable trend is the management of records. Business based on modern web 2.0 encourages cloud usage, and it is almost impossible to talk about online work without talking about the cloud (Stuart and Bromage 2010), which implicitly also makes the cloud a topic of interest for the archival community. Katherine Stuart and David Bromage (2010) present a set of problems related to cloud computing and records management: (1) trust in records; (2) general problems related to the management of records; and (3) the fact that the storage location of the records is unknown.

This last problem of where the files are stored is not solely an archival problem (Benson, Dowsley, and Shacham 2011).

Societal changes provide another perspective on the relationship between archives and recordkeeping and computing. Since the early 1990s, changes in society due to the rapid development of information technology (IT) have been highly debated in archival science (see, for example, Cook 1997; Dollar 1992). Technical evolution does not stop, and the modern online culture and the adoption of available technologies requires new methods to be able to manage archives and records (Upward, McKemmish, and Reed 2011). Cloud computing is one of these new technologies affecting the archival domain. The Internet and new technologies have also established a more mobile work trend, which Sari Mäkinen (2013) takes as the departure point for her work. She argues that the mobile worker and the new ways of using mobile technology put archives and record management to the test. One can argue that modern mobile workers are also a driving force for cloud storage and cloud usage within the records management domain (Mäkinen and Henttonen 2011; Mäkinen 2013). Archival theory rests upon the idea of provenance, and, according to Mohamed Sakka, Bruno Defude, and Jorge Tellez (2010), provenance is even more challenging to achieve in the cloud compared to relational databases, for example. This survey of the field indicates that there are several challenges for archival science regarding cloud computing and its components. One of the most obvious problems is how to trust digital records (see, for example, Duranti and Rogers 2012) and those in the cloud are even more problematic.

This article will focus on how trust in various cloud solutions can be understood from the perspective of archivists, who have previously been seen as guardians of trustworthy records. However, when more records are stored in the cloud, archivists cannot be the same kind of "guardians" that they were with analogue and paper-based records—they have a different role. This article does not aim to focus on how to make digital records trustworthy; trust comprises more than a technical solution. Trust involves actors, and this article investigates the archivists as actors. The purpose of this article is therefore to explore whether cloud computing has changed the archivist's role and how modern archivists relate themselves and their work to problems and challenges that spring from the cloud.

## Cloud service perspectives

In this article, the model defined by the NIST has been used, serving as a guide for characterizing the cloud: "This cloud model is composed of five essential characteristics, three service models, and four deployment models" (Mell and Grance 2011, 2). The essential characteristics include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The model presents three different services from the cloud: SaaS; PaaS; and IaaS. Finally, the four deployment models are private cloud, community cloud, public cloud, and hybrid cloud. The service models' and the deployment models' internal relationship with each other, together with the characteristics of the

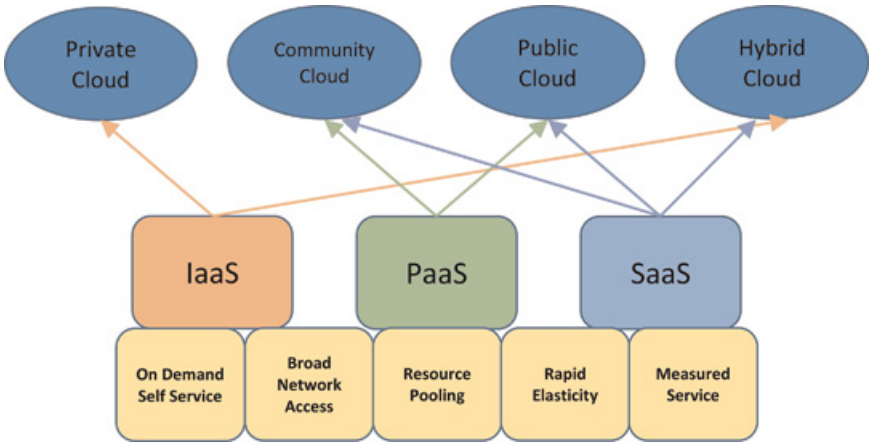



*Figure 1:* Cloud characteristics and the relationship between deployment models and service models (Vizcayno n.d.)

cloud (derived from the earlier definition) have been used. Their relationship is presented in Figure 1.

According to the NIST, five essential characteristics make the cloud what it is: (1) on-demand self-service, which allows users to access as many computing capabilities as they need; (2) broad network access, so that a user can access the cloud from any machine that has a connection to the Internet; (3) resource pooling, which makes the cloud into a multi-tenant model, supporting multiple users at the same time; (4) rapid elasticity, so that users can change the amount of computing resources they need at any time and the cloud will instantly expand to support their needs; and (5) measured service, so that how much a user utilizes is precisely measured in terms of storage, processing, bandwidth, and so on, and these resources can be monitored, controlled, and reported to the users, who are only charged for what they need, using a pay-as-you-go model, which reduces costs in most cases.

## Perspectives of trust in archival science

Although this article does not focus on making digital records in the cloud trustworthy, it is relevant to understand the perspective of trust that has influenced this research. Historically, archives have been seen as the guardians of evidence, which requires trustworthy records (Duranti 1996). It is possible to interpret the archives as black boxes in which the records are always kept in a secure environment, guaranteeing the trustworthiness and evidential value of every single record. The trustworthiness of records is seldom questioned, even when the records are removed from their origin, as demonstrated in the cases of WikiLeaks and the whistleblower Edward Snowden.

The impact of Snowden's information leaks seems to be related to citizens' trust in government records, which is in turn rooted in a long tradition of

managing and keeping records and archives. No one actually questioned the correctness of the leaked information. This example illustrates citizens' trust in public records, despite the fact that these records were extremely vulnerable to manipulation outside their original context and custody. In the digital world, records are no longer necessarily in the custody of the archive. Only part of the record is captured as a record, and digital signatures or other technical measures used to guarantee authenticity often do not exist. This situation makes it more pressing to understand how trust is created in the digital world. It also helps to understand how trust can be lost. The current move toward open data, reuse of public sector information, and cloud storage increases the importance of understanding how trustworthy and reliable records can be ensured whenever and wherever they move in the new, networked environment.

Trust is a fundamental concept in archival science, and it is extremely important that records can be guaranteed to be trustworthy. However, researchers interested in all three dimensions of trust (individual, organizational, and temporal) are rarely found. The relationship between records, trust, and evidence has been an issue for discussion among archival scholars influenced by cultural, technological, legal, and philosophical trends. When viewing records as impartial evidence, the records derive their value from the manner in which they were created as "by-products of activity rather than conscious players in the activity itself" (Trace 2002, 139). However, trust must also be understood and seen in relation to what constitutes the record. Anneli Sundqvist (2011, 277) explains that records are both instruments of trust and objects to be trusted. The main difference between records that are digital and those that are paper/analogue is that the electronic records are only logical, not physical, objects. According to Sundqvist, trust is relational since it always involves someone who trusts, and trust, rather than being the result of rational calculations, works as "a substitute for explicit knowledge" (279). Time itself is a challenge since records must be able to be trusted even after their original context is gone, which is why formalities have been developed: for example, date, signature (internal), requirements of custody (external), and so on (284). In the digital environment, trustworthiness is often achieved by technical solutions such as digital signatures (Duranti and Rogers 2012), but there are also various forensic technologies that can demonstrate whether records are trustworthy.

In a digital environment such as the Internet, it is natural that trust in information has become more and more relevant (Kelton, Fleischmann, and Wallace 2008), particularly since the use of Internet technologies is now fully embedded in modern society. Kari Kelton, Kenneth Fleischmann, and William Wallace (2008) list one simple way of categorizing trust in four levels: individual, interpersonal, relational, and societal. Morten Hertzum et al. (2002) show that trust in information is an intertwined mix of people, documents, and virtual agents affecting trust. In more management-focused literature, trust is seen as being between individuals and is often presented as an outcome of a process in which actors come to trust each other (Blomqvist 1997). It is obvious that trust is a very multifaceted concept, and a large sample of research measuring trust

between organizations was completed by Risto Seppänen, Kirsimarja Blomqvist, and Sanna Sundqvist (2007).

## Research method

The research was based upon a qualitative approach (Taylor and Bogdan 1998; Myers 2009), using twelve in-depth interviews with archivists. Two criteria were used for selecting interviewees: (1) their interest in being interviewed and (2) their experience with modern archival management, which had to include digital records management. An invitation letter was sent out to available Swedish archival list servers, and an announcement was made through Twitter and Facebook, resulting in a total of fifteen replies. Of these replies, twelve were interviewed. The selection of the archivists can be characterized as adapted selection (Hartman 1998). The study was carried out in Sweden, and the interviews were done in Swedish. The interview questions were very open and focused on triggering thoughtful responses from the archivists that were interviewed. The results from the interviews were partly transcribed to support the inductive analysis process, which was used to identify patterns within the responses to each of the questions. The analysis was conducted with the help of qualitative data analysis software, Nvivo 10.

Only Swedish archivists were interviewed. Although the national bias of the research at the design phase of the study was seen as minimal, all context dependencies cannot be avoided—the cloud and usage of the cloud are not bounded by national borders. However, it should be borne in mind that this is qualitative research that does provide generalizable results, but it aims instead to present results that can be transferred to similar conditions and contexts.

## Results

The results of the interviews are structured according to the general topics elicited by the interview questions. Each topic aims to cover the overall content of the responses given by the archivists during the interview.

### *Trust and the cloud in general terms*

The interviews all started with a general question about trust and the cloud and how each archivist spontaneously thought about trust and the cloud. This was a question that triggered a lot of response from the interviewees, and a couple of common areas have been identified. "Can we trust the information we store?" was the reply from one of the archivists. Others gave similar answers, with problems related to trust being a common theme. Can we trust that the information stored in a cloud service is stored in a correct way; can we trust the service provider; and can we trust that the information is kept within the national borders? In this case, trust is a multifaceted term focusing on both the records and the service provider. Many archivists considered it important to set up a contract or agreement that increases trust. Focusing on information security and the management of information security is one strategy that implicitly increases trust.

Another more general problem that was identified is the fact that the cloud is intangible since physical components of the cloud service are not visible to the customer (that is, the servers are placed at a location hidden from the customer). This intangibility makes trust more difficult to define and discuss. In a physical archive, the door could be opened to inspect the archival records yourself, and if it was well kept it is easier to trust the archival provider. With the cloud, you do not fully know what to trust because there is limited competence and knowledge about what a cloud is and how it works. Some of the archivists who were interviewed also said that the cloud is probably more trustworthy than other alternatives just because the service providers are professionals, and the problem with trust is more related to the fact that the providers are not clearly identifiable.

### *Challenges*

New technical solutions and new technical innovations adopted by organizations and archivists might result in different challenges for the archival profession to solve. Many of these are related to problems, which the interviewed archivists defined as 'challenges'. They are listed below because they are difficult to categorize.

- *Long-term perspective.* How long can cloud service providers guarantee the service? How can we guarantee that the information stored in a cloud service today can also be accessible and useful in the future?
- *Knowledge.* Archivists do not have enough competence and knowledge about cloud services and IT to be able to define the requirements for a cloud service. There is a risk that due to this low level of knowledge the organization's IT department will assume responsibility for the written contract between the cloud service provider and the organization.
- *Black box syndrome.* Even if the cloud service provider gives several customer business references, they still resemble a black box service. For a potential customer, it is very difficult to verify and check that the cloud service provider really can do what they claim. It is also very difficult to check that the cloud service provider has the relevant technical systems for long-term preservation.
- *Information security.* Managing information security is a challenge when information is managed in a cloud service and the "information owner" does not have physical access to the information.

### *Trust in the cloud provider*

The introduction question presented the major problem of trust in the cloud provider. However, trust is not a universal term, so the ways in which trust in the cloud provider can be understood will be examined. After analysing the interviews, a set of very clear categories related to trust became visible. First, trust is related to something that can best be described as a relationship with the cloud provider—a relationship that exists between the user and the provider of the cloud service. If the organization has had some previous and historically successful business with the cloud service provider, it was claimed that trust will

increase. In other words, a common history is often positive. Trust is also expected to be easier to achieve if the cloud service provider is close to the client organization. In other words, the perception of trust can be related to physical distance between the customer (the organization) and the cloud service provider.

Second, trust as concept can also be divided into sub categories. "Can we trust the cloud service provider not to give away the stored information to someone else?" was one of the archivists' spontaneous replies to the question. Another question was: "can we really trust that the cloud service provider knows what they are doing, that they have the relevant competence about Swedish archival regulations?" These two different trust perspectives relate to the cloud service provider but have different foci. One-third of the interviewed archivists mentioned the whistle-blower Edward Snowden as one example of why it is problematic to trust a cloud service provider. You do not really know with whom they will share the information.

### *Trust and the record*

When talking about cloud services, it is natural to include the aspects of trust related to the artefact, the information object that is kept in the cloud—that is, the records that are managed. The interviewed archivists all agreed that trust in relation to records in the cloud is very similar to the problems that exist with all digital records. The problem with trustworthy records is that in cloud services an external partner manages the records. The record is digital, and, therefore, the same kind of problems relating to trust can be identified in these records as in other digital records. It is challenging to guarantee that the record fulfils the quality criteria of authenticity, integrity, completeness, and usability. However, there is almost a paradox with trust because if you do not trust the record, then the whole business idea of the cloud is useless. Some of the archivists also said that the trustworthiness of records stored in the cloud might even be higher than with records stored and managed in-house by an IT department with doubtful competence.

### *Competence needs*

Every interviewed archivist agreed that the phenomenon of the cloud was here to stay and that it would be very problematic to manage archival issues inside the cloud without specific and new knowledge and competences. Three major competence areas were identified during the interviews. These competences exist side by side and are not mutually exclusive; on the contrary, they are intertwined:

1. *IT knowledge.* Archivists should increase their IT knowledge. Some of the archivists proposed that the modern archivist should have a more IT-based toolbox—that is, they should have basic knowledge in information systems, system science, databases, and so on. Knowledge in information security was also identified as being relevant. Increased IT competence would allow archivists to communicate better with cloud service providers, including supporting communication between archivists and IT professionals.

2. *Requirement engineering.* Requirement engineering is seen as the competence to identify the user, organization, and IT requirements for the management of digital records in a cloud environment. All archivists agreed that they needed competence for specifying requirements. This competence requires knowledge about cloud services as technology.
3. *Agreement/contract design.* Competence to work with agreements and contracts is also necessary. If the organization aims to use cloud solutions, it is important to finalize an agreement between the organization and the cloud service provider. This cannot be left to lawyers or IT professionals. Archival requirements also need to be embedded in the agreement.

### *Archivists' new responsibilities*

Given the new competences that are needed, a relevant follow-up question is whether archivists in modern organizations have acquired new responsibilities as a result of the increased use of cloud services. Previously, archivists were seen and presented as guardians of trustworthy records, but it is absolutely natural that this picture can and must be changed. One of the archivists said: "The archivist has become more of a guardian of the entire organization's archival interests than merely guardian of the records." This quotation is a comprehensive summary of the new responsibilities that became visible during the interviews. Proactivity is another word that explains the archivists' expanded responsibilities. Such proactivity becomes operational when the archivist needs to specify requirements, draft agreements, and contribute to writing the contract between the organization and the cloud service provider. He or she may also need to develop rules and regulations supporting the organization's work with various cloud services. The new proactive approach makes the archivist a generalist as well as an expert.

### *Will the role of archivists change?*

The need for archivists to be proactive and broaden their responsibilities beyond that of a guardian changes their role. The archivist is now responsible for how information is managed and controlled—they are no longer merely guardians but, rather, more of a controller responsible for information management. When it comes to cloud services, this audit function becomes more important, ensuring that information in departments in an organization is managed and controlled according to the regulations and requirements. Some of the interviewed archivists saw an opportunity for the archivist to work together with the IT department to set up a new cloud audit service to guarantee that organizational information assets kept in the cloud are kept according to organizational requirements.

Even if the cloud changes the role of the archivist, all archivists interviewed in this study claimed that responsibility for providing records upon request will still be the archivist's responsibility. Another role that will not change is responsibility for appraisal and archival description, although its craftsmanship will change due to the cloud environment.

### *Reasons for using the cloud*

The primary reason for using different cloud services relates to costs. Half of the archivists replied spontaneously that the primary motive for using cloud services was because of their low cost and the need to save money. However, after discussing this topic with them in more depth, a more nuanced picture became clear. The price of the service is still important, of course, but the cost is also related to the service level. When organizations set up their own services in-house or hosted on controlled servers, it is not completely clear what the cost will be in in relation to the service. However, by using cloud services, the majority of the interviewed archivists said that they knew what they got for a defined cost. Service/cost is clearer with cloud services.

Yet cost is not only related to cost for the service—that is, the storage and management of stored data. Competence is not cheap, and by using cloud services organizations can minimize the internal competence required. An IT department does not need to be an expert in setting up advanced storage solutions that will fulfil archival requirements. However, organizations that do not have this competence can also choose the cloud merely because they do not have to have the competence in-house. The technical evolution regarding advanced IT and data and records storage is growing quickly, and it can be impossible to guarantee that smaller organizations will have the right competence for managing their archives.

Citizens and external users were also cited as a reason for using the cloud. The archivists argued that there is a trend in public organizations to be more service oriented, and trends such as open data make public organizations more eager to test and use cloud-based services. Many citizens are used to accessing services they use themselves, such as DropBox, Box, iCloud, and GoogleDrive, from any device, and this is another reason why public authorities are going for cloud solutions. The citizens request easy access and this access motivates cloud usage, which makes it easier to access and reach data, information, or records that are stored in such services. Staff within public organizations also use cloud solutions privately and this use creates an organizational-bounded desire for such services. Easiness, smooth access, and flexibility are arguments that were presented during the interviews.

The last reason for using the cloud, which was presented by many of the archivists, was ideological. Many public authorities have decided that they should not host any IT in-house and that all such technology should be bought in as a service. There is a trend to streamline public work, contracting out as much as possible. IT, economy, human resource management, and archives are all examples of support processes that can be put in the cloud instead of being managed by the organization itself.

### *Risk taking*

The interviewed archivists were asked whether they thought that organizations and individuals tend to become more willing to take risks concerning cloud services. They were asked to compare this idea both to other digital record

management and archival management technologies and also to purely analogue management. Eight of the archivists agreed that they tend to take more risks, as individuals and in their organizations, when it comes to the use of various cloud services. It is hard to clearly identify the underlying reasons, but some tendencies can be presented. First, risk taking is argued to result from low competence and juridical and IT knowledge among archivists as well as among decision makers primarily. Some of the archivists discussed risk taking as an effect of a more negligent use of information in modern society. Another aspect of risk taking is that those who have become used to cloud services privately have adopted more risk-tolerant behaviour since the easiness of cloud services has made them willing to take more risks.

Some of the archivists argued that cloud services could, on the contrary, be more secure than other alternatives because the cloud service providers are experts in what they do, while small organizations' IT departments may not have the necessary expertise. The long-term perspective was a common challenge for all archivists, who thought that none of their organizations really tried to understand the risks connected to the requirements of preserving records over the long term. The concept of the cloud is not easy to grasp, and, therefore, the risks that organizations and individuals are willing to take may be interpreted as more risky than they are in reality. However, in-house digital storage is also risky, and the risks related to physical archives are very seldom discussed. In the worst case, physical archives can be more risky than the cloud. But the archivists who were interviewed all claimed that risks with the cloud are also more fuzzy and difficult to understand.

### *Rules and regulations*

Opinion was divided among the interviewees on whether the regulations and the current National Archives of Canada Act support the archivists in their work with the cloud.[1] Two clear opposing perspectives became visible. The first was that the rules and regulations are good enough, and those problems that exist depend entirely on how each organization applies the regulations. This perspective rests upon assumptions wherein regulations are seen in general terms. The second perspective is totally opposite, where the new phenomena of cloud service and digital records are seen as being so radically new and different that current rules and regulations are extremely out of date. Proponents of both perspectives made it clear that they considered it necessary to design practical guidelines based on the current regulations.

### *SaaS, PaaS, or IaaS*

The last section of the interviews focused on trying to see which of the three service models might be most popular. The archivists all said that the service models do not, in reality, have borders that are as clear as the NIST (National Institute of Standards and Technology 2009) states. They said that their experience is rather that these service models are intertwined. Not one of the interviewed archivists worked at an organization that had used PaaS and IaaS on their own.

On the other hand, all had some experience in using SaaS, but this was often combined with IaaS. In the Swedish context, the terms Saas, PaaS, and IaaS have not been fully adopted by the archival community, and the interviewed archivists could neither say whether their IT departments had used these terms.

## Concluding remarks

The purpose of the research presented in this article was to investigate whether cloud computing has changed the archivist's role and how modern archivists relate themselves and their work to problems and challenges that spring from the cloud. Based upon the interviews carried out in this research, new knowledge is presented. The archivists interviewed for this article described how their role has changed due to the effects of cloud computing and the introduction of cloud services in the domain of archival science. Their role has previously been more reactive—that is, to act when the information has already been created, which is impossible with digital records in general but even more problematic when it comes to cloud services. A proactive approach is proposed in which the archivist protects the organization rather than the archival records. The proactive archivist makes sure that requirements are updated and that the contract and agreement between the organization and the cloud service provider is correct.

Cloud services and cloud computing are different from other digital records management and archival management techniques. This distinction has had an impact upon trust as well. Trust in relation to cloud services is complicated and this research shows that trust consists of several dimensions, and, therefore, trust is not something that can be easily achieved with technical solutions alone. This research also indicates that there has been a change in organizations' willingness to take on risk and that the cloud services currently on offer provide easier and cheaper solutions for organizations.

The problems presented by Stuart and Bromage (2010) that relate to cloud computing and records management have been only partly confirmed by this research. The problems they outline include (1) trust in records, (2) general problems with the management of records, (3) the unknown location of the stored records. The first problem that Stuart and Bromage (2010) present about trust in records has not been fully confirmed by our research. As described previously, the problem of trust in the cloud service provider is still seen as a larger issue. The problem with the general management of records has also not been confirmed other than by several comments about general challenges in records management. The third problem, however, has been confirmed by our research.

The research presented in this article will be followed by a larger questionnaire-based study that will aim to reach a larger sample of archivists and further explore how it is possible to interpret issues concerning the cloud and trust. This future research will also aim to identify the many dimensions of trust in relation to cloud services. However, instead of seeing the cloud as a problem, this research will support the perspective that the cloud is actually a starting point for the creation and establishment of new, proactively driven archival practice that in turn supports the development of new, relevant, and up-to-date methods.

**Notes**

1. National Archives of Canada Act, RSC 1985, c 1.

**References**

Askhoj, J., M. Nagamori, and S. Sugimoto. 2011. ''Archiving as a Service: A Model for the Provision of Shared Archiving Services Using Cloud Computing.'' Proceedings of the 2011 iConference, Seattle, WA. http://dx.doi.org/10.1145/1940761.1940782.

Askhoj, J., S. Sugimoto, and M. Nagamori. 2011. ''Preserving Records in the Cloud.'' *Records Management Journal* 21 (3): 175–87. http://dx.doi.org/10.1108/09565691111186858.

Benson, K., R. Dowsley, and H. Shacham. 2011. ''Do you know where your cloud files are?'' Proceedings of the Third ACM Workshop on Cloud Computing Security Workshop, Chicago, IL. http://dx.doi.org/10.1145/2046660.2046677.

Blomqvist, K. 1997. ''The Many Faces of Trust.'' *Scandinavian Journal of Management* 13 (3): 271–86. http://dx.doi.org/10.1016/S0956-5221(97)84644-1.

Cook, T. 1997. ''What Is Past Is Prologue: A History of Archival Ideas since 1898, and the Future Paradigm Shift.'' *Archivaria* 43: 17–63.

Dollar, C.M. 1992. *Archival Theory and Information Technologies: The Impact of Information Technologies in Archival Principles and Methods.* Macerata, Italy: University of Macerata.

Duranti, L. 1996. ''Archives as a Place.'' *Archives and Manuscripts* 24 (2): 242–56.

Duranti, L., and C. Rogers. 2012. ''Trust in Digital Records: An Increasingly Cloudy Legal Area.'' *Computer Law and Security Review* 28 (5): 522–31. http://dx.doi.org/10.1016/j.clsr.2012.07.009.

Ferguson-Boucher, K., and N. Convery. 2011. ''Storing Information in the Cloud: A Research Project.'' *Journal of the Society of Archivists* 32 (2): 221–39. http://dx.doi.org/10.1080/00379816.2011.619693.

Hartman, J. 1998. *Vetenskapligt tänkande: från kunskapsteori till metodteori*. Lund: Studentlitteratur.

Hertzum, M., H.H.K. Andersen, V. Andersen, and C.B. Hansen. 2002. ''Trust in Information Sources: Seeking Information from People, Documents, and Virtual Agents.'' *Interacting with Computers* 14 (5): 575–99. http://dx.doi.org/10.1016/S0953-5438(02)00023-1.

Kelton, K., K.R. Fleischmann, and W.A. Wallace. 2008. ''Trust in Digital Information.'' *Journal of the American Society for Information Science and Technology* 59 (3): 363–74. http://dx.doi.org/10.1002/asi.20722.

Mäkinen, S. 2013. '''Some records manager will take care of it': Records Management in the Context of Mobile Work.'' *Journal of Information Science* 39 (3): 384–96. http://dx.doi.org/10.1177/0165551512471934.

Mäkinen, S., and P. Henttonen. 2011. ''Motivations for Records Management in Mobile Work.'' *Records Management Journal* 21 (3): 188–204. http://dx.doi.org/10.1108/09565691111186867.

Mell, P., and T. Grance. 2011. *The NIST Definition of Cloud Computing*. Gaithersburg, MD: National Institute of Standards and Technology; http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Myers, M.D. 2009. *Qualitative Research in Business and Management*. London: SAGE.

National Institute of Standards and Technology (producer). 2009. *Definition of Cloud Computing*. http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf.

Sakka, M., B. Defude, and J. Tellez. 2010. ''Document Provenance in the Cloud: Constraints and Challenges.'' In *Networked Services and Applications: Engineering, Control and Management*, vol. 6164. ed. F. Aagesen and S. Knapskog, 107–17. Berlin: Springer. http://dx.doi.org/10.1007/978-3-642-13971-0_11.

Seppänen, R., K. Blomqvist, and S. Sundqvist. 2007. ''Measuring Inter-Organizational Trust: A Critical Review of the Empirical Research in 1990–2003.'' *Industrial Marketing Management* 36 (2): 249–65. http://dx.doi.org/10.1016/j.indmarman.2005.09.003.

Stuart, K., and D. Bromage. 2010. ''Current State of Play: Records Management and the Cloud.'' *Records Management Journal* 20 (2): 217–25. http://dx.doi.org/10.1108/09565691011064340.

Sundqvist, A. 2011. ''Documentation Practices and Recordkeeping: A Matter of Trust or Distrust?'' *Archival Science* 11 (3-4): 277–91. http://dx.doi.org/10.1007/s10502-011-9160-3.

Taylor, S.J., and R. Bogdan. 1998. *Introduction to Qualitative Research Methods: A Guidebook and Resource*, 3rd edition. Chichester, NY: Wiley.

Trace, C.B. 2002. ''What is recorded is never simply 'what happened': Record keeping in modern organizational culture.'' *Archival Science* 2 (1-2): 137–59. http://dx.doi.org/10.1007/BF02435634.

Upward, F., S. McKemmish, and B. Reed. 2011. ''Archivists and Changing Social and Information Spaces: A Continuum Approach to Recordkeeping and Archiving in Online Cultures.'' *Archivaria* 72: 197–237.

Vizcayno, D.C. n.d. Danielito C. Vizcayno Blogs. http://dcvizcayno.wordpress.com/2012/04/13/cloud-computing-tips-for-financial-industry/.